2018 年第 3 期　总 130 期
ISSN 1674-9804　CN 31-1614/V

DOI：10.19416/j.cnki.1674－9804.2018.03.023

RTCA/DO-331 标准研究

Research on RTCA/DO-331 Standard

居　慧 / JU Hui
（上海飞机设计研究院，上海 201210）
（Shanghai Aircraft Design and Research Institute，Shanghai 201210，China）

摘　要：
为推动基于模型的开发和验证技术的发展，同时为了给机载软件基于模型的开发和验证活动提供合格审定指南，美国航空无线电委员会于 2011 年发布了 DO-331《基于模型的开发和验证》标准，作为对 DO-178C《机载系统和设备合格审定中的软件考虑》标准的补充。该文主要从 DO-331 文档的组织架构编排，模型的使用和分类，基于模型研制相关的软件生命周期过程、数据和符合性验证目标几个方面对其进行了提炼和解读，可帮助应用该标准的人员快速理解文档的核心内容，并把握基于模型的开发和验证相关的合格审定关注点，从而在项目实施过程中更好地表明适航符合性。
关键词：DO-331；基于模型的开发和验证；机载软件；合格审定
中图分类号：V233.7　　**文献标识码：**A　　**OSID：**

[**Abstract**] In order to facilitate the progress of the Model-Based Development and Verification (MB) technology, and also provide the certification guidance for the airborne software MB activities, Radio Technical Commission for Aeronautics (RTCA) released DO-331 Model-Based Development and Verification standard, as a supplement document to the DO-178C Software Considerations in Airborne Systems and Equipment standard in 2011. This Paper provides the abstraction and explanation for the DO-331 from the aspects of its structure organization, models usage and category, MB related software lifecycle processes, data and certification objectives, which can help people who use this standard understand its core content quickly and capture the certification concerns of MB, therefore demonstrate the certification compliance well during the program implementation process.
[**Keywords**] DO-331; model-based development and verification; airborne software; certification

0　引言

当前在民用航空领域，越来越多的机载设备供应商在采用基于模型的开发和验证（Model-Based Development and Verification，简称 MB）这种基于结构化分析和设计的方法研制机载软件，因为模型的使用可以带来一些便利，例如支持自动化代码的生成，支持仿真手段的使用等。自 DO-178B[1] 发布至今，业内已经在基于模型的开发和验证技术的应用和支持工具研发方面积累了一定的经验，而随着此项技术在航空关键系统软件的应用逐渐增多，有很多问题需要考虑以确保满足系统安全性和完整性的要求。

由于 DO-178C[2] 不是一份针对特定方法或特定技术的指南，因此采用 MB 方法开发的机载软件在直接表明对于 DO-178C 某些目标的符合性方面存在困难或不清晰的情况，甚至有一些空白。为了给基于模型的开发和验证活动的合格审定提供明确的指南，也为了推进这项技术在工业界的发展，美国航空无线电委员会（Radio Technical Commission for Aeronautics，简称 RTCA）于 2011 年以 DO-178C 补充文档的形式发布了 1 份标准 DO-331[3]《基于模型的开发和验证（对于 DO-178C 和 DO-278A 的补充）》。该份补充文档是在 DO-178C 的基础上针对 MB 技术对原先机载软件合格审定指南的扩展。2013 年，美国联邦航空局（Federal Aviation Administration，简

称 FAA)发布咨询通告 AC20-115C《机载软件保证》认可包括 DO-331 在内的五份 RTCA 标准作为机载软件满足适航规章可接受的符合性方法。

由于 DO-178C 发布的时间不长,目前仅在一些新的飞机项目中应用为符合性方法,还未形成成熟的可借鉴的审定实践经验,对于该标准及其补充文档(包括 DO-331 在内)的研究具有重要意义,有助于申请人在项目研制过程中更好地理解和贯彻合格审定要求,成功表明适航符合性。

1　DO-331 标准的文档架构

DO-331 标准在主要章节的编排组织形式上与 DO-178C 保持一致,覆盖了整个软件研制流程,但为了以示区分,所有章节均采用以 MB 作为前缀的编号规则。标准的主体内容继承了 DO-178C,在此基础上补充了有关基于模型的开发和验证的内容,包括生命周期数据和相应的目标,并在附录中增加了应用 DO-278A[4] 和 DO-331 时不同等级的软件生命周期过程的目标和输出的汇总表格,以及常见问题解答和讨论专题。为了最大程度地减少与 DO-178C 的重复信息,DO-331 中仅对 DO-178C 受影响的章节进行了更新,对于描述内容无差异的章节,直接声明对应的 DO-178C 章节内容没有变化。其中,从 DO-178C 完全继承的内容统一采用斜体字表示,新增或修改的内容为正常字体表示。相比 DO-178C,DO-331 的专有内容如表 1 所示。

表 1　DO-331 专有内容一览

章节编号	章节名称	内容概述
MB.1.6	基于模型的开发和验证的特性	简述了建模技术,定义了模型分类,并提供了模型使用样例
MB.4.4.4	仿真环境	描述了仿真环境规划所包含的活动
MB.6.7	设计模型的模型覆盖分析	描述了针对设计模型所进行的模型覆盖分析的目的和活动,包括模型覆盖分析的准则确立以及模型覆盖缺陷的解决方案
MB.6.8	模型仿真	描述了针对模型验证的模型仿真和针对可执行目标代码验证的模型仿真可以满足的验证目标,执行的活动以及仿真用例、程序和结果的开发、评审和分析
MB.11.23	软件模型标准	定义了作为生命周期数据之一的软件模型标准应该包含的内容
ANNEX MB.C	DO-278A 不同软件等级过程目标和输出	在 DO-278A 附录 A 的基础上,提供了采用基于模型的开发和验证方法生成 CNS/ATM 系统软件相关的目标、活动和输出的表格
APPENDIX MB.B	常见问题解答和讨论专题	总结了理解 DO-331 的一些常见问题和解答,并提供了有关基于模型的开发和验证的一些讨论专题

2　模型的使用和分类

DO-331 中介绍了以下两类模型:

1)规范模型(Specification Models):描述提供软件组件功能、性能、接口或者安全性特性的抽象表示的高级别需求;

2)设计模型(Design Models):规定了软件组件内部的数据结构,数据流和/或控制流,包含低级别需求和/或软件架构。

DO-331 中明确强调模型不能同时划分为规范模型和设计模型,并且依据当前的一些工业实践提供了模型使用的样例,如表 2 所示。由表 2 可看出,设计模型使用的场景更为广泛,但不管模型如何使用,都需要满足相应的符合性目标。

表 2　模型使用样例

生成软件生命周期数据的过程	MB 样例 1	MB 样例 2	MB 样例 3	MB 样例 4	MB 样例 5
系统需求和系统设计过程	分配到软件的需求	模型开发依据的需求	模型开发依据的需求	模型开发依据的需求	模型开发依据的需求
软件需求和软件设计过程	模型开发依据的需求	规范模型	规范模型	设计模型	设计模型
	设计模型	设计模型	文本描述		
软件编码过程	源代码	源代码	源代码	源代码	源代码

3　MB 相关的软件生命周期过程

3.1 软件计划过程

如果计划采用基于模型的开发技术，软件计划过程除了需要满足 DO-178C 中定义的目标和活动外，还需满足以下几点：

1）识别出将由模型描述的软件生命周期数据，例如：需求数据或者设计数据，所有开发模型应按照上述模型的分类进行划分；

2）识别出将采用的验证模型的方法，包括对于设计模型的模型覆盖分析准则的定义；

3）应生成软件模型标准，描述采用的建模技术以及对于每类模型适用性的理由；

4）规划模型仿真环境，定义当采用模型仿真器执行验证活动时可能采用的方法、工具、程序和操作环境，主要活动包括：

（1）确定模型仿真器是否需要鉴定，评估的准则参考 DO-331MB.12.2 节（工具鉴定）；

（2）明确说明模型仿真器的性能和限制，包括预期的使用以及对于检测错误和验证功能的能力的影响；

（3）评估仿真环境更改的影响，考虑按照 DO-331 第 MB.6 章（软件验证过程）和 MB.12.1.3 节（更改应用或开发环境）中的指南进行重新验证。

3.2 软件开发过程

如果在软件开发过程中采用了基于模型的方法，基于 DO-331 中对于规范模型和设计模型的定义，所有高级别需求相关的目标和活动适用于规范模型中包含的需求或者设计模型开发所依据的需求，所有软件架构和低级别需求相关的目标则适用于软件设计模型中包含的软件架构和需求。此外，对软件需求和设计过程的目标和活动会有一些附加要求，主要体现为：

1）如果高级别需求采用规范模型予以描述应标识出所有不代表软件需求并且不作为后续软件开发过程或者活动的输入的模型元素；

2）如果低级别需求和/或架构采用设计模型予以描述，应标识出所有不代表软件需求或软件架构并且不作为后续软件开发过程或者活动的输入的模型元素；

3）如果软件需求或软件架构采用模型予以描述，模型应遵循软件模型标准并具有可追溯性、可验证性和一致性，所有模型元素应按照软件模型标准中的描述进行分类；

4）如果计划开发设计模型，对应该模型的软件高级别需求应包含足够的细节以支持后续设计模型的实现和验证。

3.3 软件验证过程

如果采用了基于模型的开发方法，除了满足对于软件需求验证、设计验证、代码验证和测试有关的基本目标外，鉴于模型的研制特性，软件验证过程中还需关注：

1）开发的模型是否符合软件模型标准，是否对偏离标准的方面进行了解释说明；

2）如果高级别需求采用规范模型描述，低级别需求和规范模型之间的追溯性；

3）如果低级别需求采用设计模型描述，源代码和设计模型之间的追溯性；

4）如果软件开发过程中采用了设计模型，应按照 DO-331MB.6.7 节中的指南开展模型覆盖分析活动。

模型覆盖分析活动主要包括：

1）采用基于需求的验证用例，需求为设计模型开发所依据的需求；

2）确认通过验证用例所达到的设计模型的覆盖度是否与计划过程中定义的模型覆盖准则一致，在不满足覆盖要求的情况下，按照 DO-331MB.6.7.2 节中的模型覆盖分析解决方案开展相关工作；

3）补充基于设计模型中的衍生需求的附加验证用例。

模型覆盖分析的准则在表述上与典型的软件结构覆盖分析的准则（语句覆盖、分支覆盖等）有所不同，如表 3 所示。表 3 中准则①到④与 DO-178C 6.4.2.1 和 6.4.2.2 节中有关覆盖分析的内容是兼容的。其中，准则 1 与软件需求覆盖相关，准则②到④与软件结构覆盖相关。

此外，DO-331 中描述了可采用模型仿真的验证方法来支持满足一些验证目标，主要内容包括：

1）针对模型验证的模型仿真，识别出了哪些软件需求和设计过程的输出的验证目标可以通过对规范模型和设计模型的仿真满足，哪些目标不能通过仿真满足，以及应执行的仿真活动；

2）针对可执行目标代码验证的模型仿真，描述了通过模型仿真和特定的分析的组合可以满足

的软件测试和测试覆盖目标以及相应的活动,其中涵盖了对于模型仿真器环境和目标计算机环境的差异分析,以及用于仿真的可执行目标代码与用于目标机的可执行目标代码之间的差异分析的要求;

3)仿真用例、程序和结果的开发、评审和分析。

表 3　模型覆盖准则样例

典型完成准则	通过验证用例和澄清(基于设计模型开发依据的需求)满足	通过验证用例和澄清(基于设计模型中包含的需求)满足
① 覆盖功能的所有特性,例如看门狗功能触发器	推荐	
② 对于状态机:覆盖所有的状态转换	推荐	
③ 对于逻辑方程:覆盖所有的决策	推荐	
④ 覆盖所有的等价类以及边界条件/奇异数值	推荐	可选
⑤ 覆盖所有的衍生需求(不能追溯到高级别需求)		推荐

3.4 其他过程

DO-331 中描述的其他软件生命周期过程,包括构型管理过程、质量保证过程以及合格审定联络过程的目标和活动与 DO-178C 中的描述并无明显差异,即采用 MB 方法对这些生命周期过程基本没有影响。

4　MB 相关软件生命周期数据

4.1 MB 专有数据

DO-331 在 DO-178C 定义的生命周期数据的基础上,增加了一个 MB 专有数据:软件模型标准。此标准应包含以下内容:

1)用于开发模型的方法和工具;

2)采用的建模语言;

3)建模语言使用的风格指南以及复杂度限制;

4)建模工具以及模型元素库的使用限制;

5)用于标识和界定模型中包含的需求的方法以及建立需求和其他生命周期数据之间的追溯性的方法;

6)用于标识和界定模型中包含的衍生需求的方法以及将衍生需求反馈到系统过程包括系统安全性评估过程的方法;

7)识别出所有不代表软件需求或软件架构并且不作为后续软件开发过程或者活动的输入的模型元素的方法;

8)通过规范模型或者设计模型表述的信息类型的技术适用性的合理解释。

4.2 其他相关数据

其他软件生命周期数据中涉及模型相关的内容主要有:

1) 软件合格审定计划 PSAC(Plan for Software Aspects of Certification,简称 PSAC):

(1)对于软件生命周期的描述应包含为满足 DO-331 目标将执行的过程和活动以及生成的数据;

(2)软件生命周期数据中应包含符合 DO-331 的数据。

2) 软件开发计划 SDP(Software Development Plan,简称 SDP):软件开发环境的描述中应包含将采用的建模方法、建模语言和建模工具。

3) 软件验证计划 SVP(Software Verification Plan,简称 SVP):

(1)验证方法之一的分析方法中应包含模型追溯性分析、模型覆盖准则和模型覆盖分析;

(2)验证方法中还应包含对于模型仿真方法的描述,包括仿真用例的选择方法,使用的仿真程序,将生成的仿真数据以及 DO-331 中 MB.6.8.1 和 MB.6.8.2 节中定义的特定限制;

(3)验证环境应包含对于模型仿真环境和工具,以及应用这些工具的指南描述;

4)软件验证用例和程序:应包含对于仿真用例和仿真程序的描述。

5)软件验证结果:

(1)应标识出模型的构型;

(2)应包含仿真的结果以及支持仿真的任何分析结果。

6)软件生命周期环境构型索引(Software Life

Cycle Environment Configuration Index，简称 SECI）：应标识仿真环境以及相关的设置。

7）软件构型索引（Software Configuration Index，简称 SCI）：标识的软件生命周期数据中应涵盖 DO-331 中 MB.2.2.1.i 到 MB.2.2.1.o 项的数据，如果存在系统构型索引并包含了这些数据，应索引至系统构型索引文档。

8）软件构型管理记录：模型的 SCM（Software Configuration Management，简称 SCM）记录的例子包括基线记录和模型元素库记录。

9）追溯性数据：如果采用模型描述高级别需求或低级别需求和/或软件架构，与模型的追溯性应提供能够展现出 DO-331 MB.11.21 节 a）到 f）项的颗粒度。

5　MB 符合性目标

DO-331 的附录 A 在 DO-178C 附录 A 的基础上，提供了采用基于模型的开发和验证方法生成机载软件需要满足的符合性验证目标，文中对应的活动描述索引和输出数据的汇总表格。这些表格中对于目标和输出的生命周期数据与 DO-331 正文中相应章节的索引关系，基于 DO-331 章节编排的调整和内容的增加进行了相应更新。除了从 DO-178C 继承的目标，考虑到模型开发和验证的特殊性，DO-331 附录 A 中的目标在 DO-178C 的基础上补充了一些模型相关的目标，详见表 4。

表 4　DO-331 新增目标

目标编号	目标描述	不同软件级别目标适用性 A	B	C	D	备注
附录 A 表 MB. A-2 # MB8	标识出不用于实现任何高级别需求的规范模型元素	○	○	○	○	
附录 A 表 MB. A-2 # MB9	标识出不用于实现任何软件架构的设计模型元素	○	○	○	○	
附录 A 表 MB. A-2 # MB10	标识出不用于实现任何低级别需求的设计模型元素	○	○	○		
附录 A 表 MB. A-3 # MB8	仿真用例是正确的	●	○	○	○	如果采用仿真的方法满足表 MB. A-3 中的有关高级别需求验证的 1、2、4 或 7 目标，应满足这 3 个目标
附录 A 表 MB. A-3 # MB9	仿真程序是正确的	●	○	○	○	
附录 A 表 MB. A-3 # MB10	仿真结果是正确的，且差异得以解释	●	○	○	○	
附录 A 表 MB. A-4 # MB14	仿真用例是正确的	●	○	○		如果采用仿真的方法满足表 MB. A-4 中的有关低级别需求和软件架构验证的 1、2、4、7、8、9 或 11 目标，应满足这 3 个目标
附录 A 表 MB. A-4 # MB15	仿真程序是正确的	●	○	○		
附录 A 表 MB. A-4 # MB16	仿真结果是正确的，且差异得以解释	●	○	○		
附录 A 表 MB. A-7 # MB10	仿真用例是正确的	●	○	○		当采用仿真的方法满足表 MB. A-6 中有关高级别需求测试的目标 1 或 2 时，应满足这 3 个目标
附录 A 表 MB. A-7 # MB11	仿真程序是正确的	●	○	○		
附录 A 表 MB. A-7 # MB12	仿真结果是正确的，且差异得以解释	●	○	○		

注：表中的○代表目标需要满足，●代表目标需要被独立满足。

6　结论

1）如果计划在民用飞机机载软件生命周期过程中采用基于模型的开发和验证技术时，在确定采用 DO-178C 作为符合性方法的情况下，也应符合 DO-331 标准中的要求；

2）DO-331 在应用时，应以 DO-178C 作为基础，综合考虑 DO-178C 和 DO-331 中的目标，同时在适用的情况下，应与 DO-178C 的其他补充文档结合使用，例如工具鉴定的相关要求应遵循 DO-330[5]《软件工具鉴定考虑》标准，才能完整地表明适航符合性。

参考文献：

[1] Radio Technical Commission Aeronautics. Software considerations in airborne systems and equipment certification: DO-178B[S]. Washington DC: Radio Technical Commission Aeronautics, 1992.

[2] Radio Technical Commission Aeronautics. Software considerations in airborne systems and equipment certification: DO-178C[S]. Washington DC: Radio Technical Commission Aeronautics, 2011.

[3] Radio Technical Commission Aeronautics. Model-based development and verification supplement to DO-178C and DO-278A: DO-331[S]. Washington DC: Radio Technical Commission Aeronautics, 2011.

[4] Radio Technical Commission Aeronautics. Software integrity assurance considerations for communication, navigation, surveillance and air traffic management (CNS/ATM) systems: DO-278A[S]. Washington DC: Radio Technical Commission Aeronautics, 2011.

[5] Radio Technical Commission Aeronautics. Software tool qualification considerations: DO-330[S]. Washington DC: Radio Technical Commission Aeronautics, 2011.

作者简介

居　慧　女,硕士,高级工程师。主要研究方向:机载软件与电子硬件管理。E-mail: juhui@ comac. cc

更　正

本刊2018 年第 2 期有以下几点需更正：

1. 第 11 页“关于飞机系统模拟试验中流量计在线校准技术的探讨”(作者:倪君菲、柯一春、盛承勋)一文中图 5 有误,更新如下：

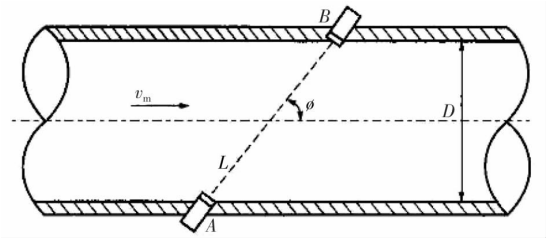

图 5　超声波在流体中传输各量示意图

2. 第 15 页“定向耦合器在天线隔离度测试中的应用”(作者:梁小亮、史剑锋、宁敏)一文中公式(7)及公式(11)有误,更新如下：

$$P_t = 10\lg(10^{\frac{(P_{13}+C_1-L')}{10}} - 10^{\frac{(P_{14}+C_1)}{10}}) - L_1 \quad (7)$$

$$D = 10\lg(10^{\frac{(P_{13}+C_1-L')}{10}} - 10^{\frac{(P_{14}+C_1)}{10}}) - (P_{23} + C_2) - L_1 - L_2 \quad (11)$$

3. 第 69 页及第 72 页“中国与‘一带一路’沿线国家航空市场现状”(作者:张楠)一文中作者及图 10 有误,更新如下：

(1)作者应为张楠、钮昊珺

(2)图 10 应为：

(a) 2013 年

(b) 2016 年

图 10　2013 年和 2016 年国内开通至沿线国家直达航线城市分布

4. 第 105 页“驾驶舱人机界面演变与发展趋势”(作者:张伟、张洁)一文中论文题名有误,更新为:一种考虑统计风的民机航程能力图绘制方法研究。